FRBB ePurse v2 on ActivCard Applet v2 on Cyberflex Access 64k v1

FIPS 140 – 2 Level 2
Cryptographic Module Security Policy
Revision 1.6

Federal Reserve Bank of Boston
FMS – US Treasury

July 20, 2006

NON-PROPRIETARY DOCUMENT

Information contained in this document is subject to change without notice. This Security Policy is a non-proprietary document and should only be reproduced without revision.

The information contained within this document was originally prepared by Jeff Colandrea for exclusive use of the Federal Reserve Bank of Boston and FMS – US Treasury. Jeff Colandrea can be contacted at Intersecting Technologies at (860)613-0713 or jcolandrea@snet.net.

TABLE OF CONTENTS

1 Introduction

This document defines the Security Policy for the "FRBB ePurse v2 on ActivCard Applet v2 on Cyberflex Access 64K v1" cryptographic module, submitted for validation, in accordance with FIPS140-2 Level 2 requirements. Included are a description of the security requirements for the module, and a qualitative description of how each security requirement is achieved. In particular, this security policy specifies the security rules under which the cryptographic module must operate.

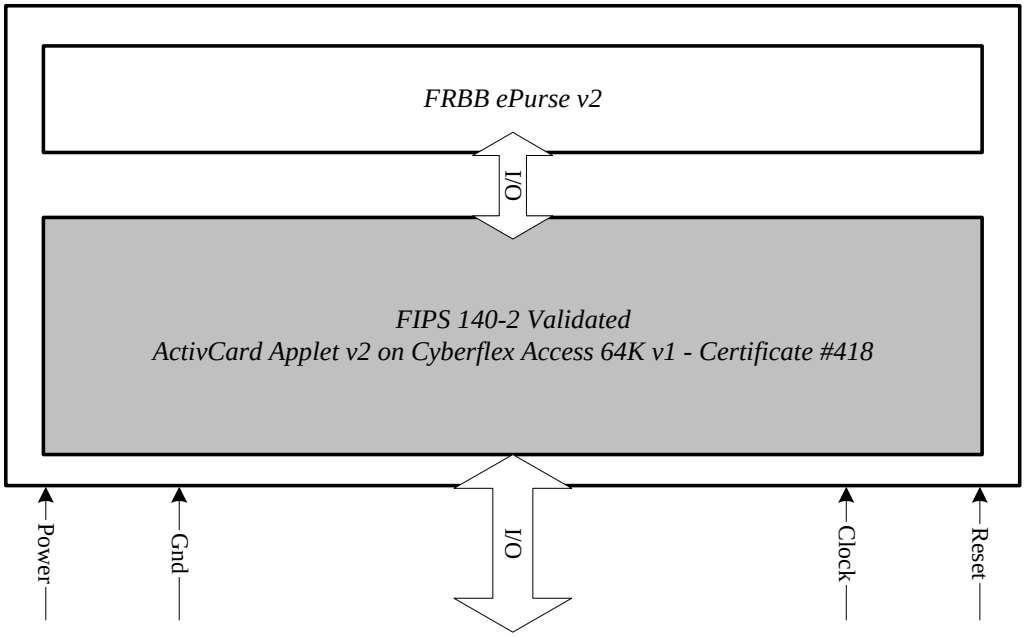

Figure 1 - FRBB ePurse v2 on ActivCard Applet v2 on Cyberflex Access 64K v1 Diagram

2 Security Level Specification

The cryptographic module is designed and implemented to meet the Level 2 requirements of FIPS140-2. The cryptographic module enforces FIPS mode of operation at all times. The individual security requirements specified for FIPS 140-2 meet the level specifications indicated in the following table.

Security Requirements Section	Level
Cryptographic module specification	2
Cryptographic module ports and interfaces	2
Roles, services, and authentication	2
Finite state model	2
Physical security	3
Operational environment	N/A
Cryptographic key management	2
EMI/EMC	3
Self tests	2
Design assurance	2
Mitigation of other attacks	2

3 Cryptographic Module Specification

This validation effort is aimed at the FRBB ePurse applet operating on the FIPS validated ActivCard Applet v2 on Cyberflex Access 64K v1. If additional applets are loaded into this cryptographic module, then these additional applets require a separate validation, and must be FIPS 140-2 validated.

The cryptographic module components are as follows:

Applet: The FRBB ePurse v2 Version: 2.0.12

Operating Platform: The ActivCard Applet v2 on Cyberflex Access 64K v1 is a FIPS 140-2 validate module (Cert. # 418)

- The Cyberflex Access 64K v1
  - Module firmware versions:
    - OS Hardmask n5 v01
    - OS Softmask n4 v02
  - Hardware version: Infineon SLE66CX640P

- The ActivCard Applet v2 (CAC framework v2.3.0C):
  - ACA applet package v2.3.0.5
  - PKI/GC applet package v2.3.1.2
  - ASC library package v2.3.0.3

3.1 FRBB ePurse v2

FRBB ePurse v2 is a stored value electronic purse applet written for the Java Card. The purse allows cardholders to purchase goods and services from merchants using authorized devices. Value can be increased as necessary using the ePurse's load feature at a designated revalue device. The purse is designed to mitigate financial risks of the funds issuer associated with the existence and use of offline value. The purse uses role-based authentication and symmetric cryptography to guard the purse against unauthorized use.

3.2 Cyberflex Access 64k v1

Cyberflex Access 64K v1 is a module from Axalto that loads and runs applets written in the Java programming language. The Cyberflex Access 64K v1 module contains a microprocessor and EEPROM to provide processing capability and memory for storing instructions and data. The module can be used to store and update account information, personal data, and even monetary value. The module, when placed in a plastic smart card housing, is ideal for secure Internet access, purchases, portable digital telephones, and for benefit programs and health care applications. The Cyberflex Access 64K v1 module, when housed in smart card housing, brings new services, as well as increased security, portability, and convenience, to computer applications.

The Cyberflex Access 64K v1 module combines the advantages of the Java programming language and cryptographic services with those of the module. Security of the Cyberflex Access 64K v1 module is derived from both the software and hardware. Data integrity and security are provided through cryptographic services, Java features, and the Systems software. In addition, the module hardware provides tamper-resistance, and tamper-evidence features that meet FIPS140-2 Level 3 physical security requirements.

The Cyberflex Access 64K v1 module contains an implementation of the Java Card ™ specification (JC) Version 2.1.1 and of the Open Platform (OP) Version 2.0.1 specification, which defines a secure

infrastructure for a post-issuance programmable cryptographic module housed in a smart card. The JC specification defines Java Card ™ Application Programming Interface (API) that can be used by applet developers to take advantage of the various on-board cryptographic services. The Cyberflex Access 64K v1 module is a "post-issuance programmable" module. It includes an on-module virtual machine interpreter that allows programs (applets) written in Java to be loaded onto the module and placed into execution. The module is considered operating in FIPS mode if the following are true; (1) only FIPS validated applets are loaded and instantiated, (2) the applets are instantiated according to the security policy described in this document. Under these conditions, the module always operates in FIPS approved mode. The module checks all validated applets and does not load any applets that do not have the correct MAC. The OP specification defines a life cycle for OP compliant modules. State transitions between states of the life cycle involve well-defined sequences of operations. Once applets are loaded and the module is initialized, external applications communicate with the Cyberflex Access 64K v1 module through a secure channel that is put into place as part of the module's initialization process when it is inserted into a card reader. The Cryptographic Officer establishes the secure channel with the Card Manager application on the module. Through the Card Manager, a secure communication pathway can be established with any of the applets on the module. Each applet can provide additional "command services" which can be accessed by external applications.

Cyberflex Access 64K v1, housed in the smart card, is an ID-1 class smart card that adheres to the various ISO/IEC specifications for Integrated Circuit Chip (ICC) based identification cards. The "cryptographic boundary" for the Cryptographic module vis-à-vis the FIPS 140-2 validation, is the "module edge". The module is comprised of the chip (ICC), the contact faceplate, and the micro-electronic connectors between the chip and contact pad.

Cyberflex Access 64K v1 is a single chip implementation of a cryptographic module. The Cyberflex Access 64K v1 chip is comprised of the following elements:

- Infineon SLE66CX640P, 8 bit micro controller,

System software is installed in Read Only Memory (ROM) as part of the chip manufacturing process (known as hard mask) and in Electrically Erasable Programmable Read Only Memory (EEPROM), for system options and additional customized software (known as soft mask).

Critical Security Parameters stored in EEPROM as part of the cryptographic module personalization operation.

3.3 ActivCard Applet v2

ActivCard Applet v2 provides significant enhancements over the ActivCard v1 Applet in service, security, and flexibility. The ActivCard Applet v2 framework is backward compatible with earlier versions of ActivCard Applets and offers a more open, stable, and flexible platform for developers to build and deploy smart card applications. ActivCard Applet v2 also complies with GSC-IS 2.1 standard.

ActivCard Applets are a modular suite of Java applets that run on a Java card. Version 2 of this suite is distinctive from Version 1 in the following ways:

- It decouples on-card application services from security management such as authentication and secure messaging, providing a more flexible, secure, and open platform for applet developers.
- It provides a flexible architecture to allow future authentication and biometric services to be added to the module without modifying existing applications.

The two applets included in the cryptographic module are:

- **Access Control Applet (ACA)** – this applet is responsible for Access Control Rules (ACR) definition, access control rules enforcement and secure-messaging processing for all card services.

Three off-card entity authentication methods – OP secure messaging, PIN, and ActivCard External Authentication are included by default in the ACA applet.

- **PKI/Generic Container (PKI/GC) Applet** – The PKI/GC Applet can be used to provide secure storage for both PKI credentials, and other data, required for implementation of card services including single sign-on applications, identity, and benefits information. This applet is responsible for RSA-based cryptographic operations using the RSA private key stored in the PKI buffer. Up to 8 buffers can be configured for each applet instance.

The applet and library package byte code is loaded in the cryptographic module memory. Note that the ASC library package consists of static utility classes only accessed by the applet and cannot be accessed directly by off-card entity.

The applets offer services to external applications, and rely on key management, secure memory management and cryptographic services, provided by the cryptographic module. The services are activated with "APDU commands" sent to the cryptographic module.

Applets depend on a unique security domain for the security configuration. This security domain can either be the Card Manager or a separate security domain. The Card Manager is itself a security domain with additional services, and applets. The Card Manager controls the global cryptographic module status.

Every security domain holds one or more security domain key sets composed of TDES keys.
The ownership of a key set allows for establishing a Secure Channel (SC) between the host and either the security domain or the security domain applets. The SC is generally used for administrative operations such as entering the application keys in the applet instances belonging to the security domain, or entering new key sets in the security domain itself. Note that a security domain key set can be used to enter a replacement key set in the same security domain – the replacement involves the deletion of the original key set.

The Card Security Controller (CSC), which owns keys sets of the Card Manager, also acts as an Applet Security Controller for all applet instances depending on the Card Manager security domain.

4 Module Ports and Interfaces

The electrical and physical interface of the cryptographic module is comprised of 8-electrical contacts from the face of the cryptographic module to the chip. These contacts conform to the specifications listed in the following sub-sections.

4.1.1 Physical Interface description

The cryptographic module supports 8 contacts that lead to pins on the chip. Only five of these are used. The location of the contacts complies with ISO/IEC 7816-2 standard. Minimum contact surface area is 1.7mm * 2.0 mm.

Contact dimensions are standard credit card compliant as per ISO/IEC 7816-1 standard:

Dimension	Value
Length	85.5mm
Width	54.0mm
Thickness	0.80mm

4.1.2 Electrical specifications

- **Specific electrical functions of the contacts:**

Contact	Function
C1	Vcc supply voltage 3 to 5V +/- 0.5V
C2	RST (Reset)
C3	CLK (Clock)
C4	Reserved for Future Use (RFU)
C5	GND (Ground)
C6	Not used
C7	I/O bi-directional line
C8	Reserved for Future Use (RFU)

- **ICC supply current:**
  Maximum value: 10 mA at 5MHz (3mA type), short time peak value according to ISO 7816-3. The communication between the card reader and the cryptographic module is based on a standardized, half-duplex character transmission, ISO 7816 protocol. Both T=0, and T=1 protocols are supported.

4.1.3 Logical Interface Description

Once electrical (physical) contact, and data link layer contact are established between the cryptographic module and the card reader, the cryptographic module functions as a "slave" processor to implement and respond to the card reader commands. The cryptographic module adheres to a well-defined set of state transitions. Within each state, a specific set of commands is accessible.

5 Roles and Services

5.1 ActivCard Applet v2 on Cyberflex Access 64k v1 module roles

The ActivCard Applet v2 on Cyberflex Access 64k v1 defines four distinct roles that are supported by the on-module cryptographic system; Card Security Controller (CSC) role, Applet Security Controller (ASC) role, Application Operator role, and Card Holder role.

5.1.1 ActivCard Applet v2 on Cyberflex Access 64k v1 User Roles:

- **ActivCard Applet v2 on Cyberflex Access 64k v1 Card Holder Role** - The Card Holder role is responsible for insuring the ownership of his cryptographic module, and for not communicating his PIN to other parties. An applet authenticates the Card Holder by verifying his PIN.

- **ActivCard Applet v2 on Cyberflex Access 64k v1 Application Operator Role** – The Application Operator role represents an external application requesting the services offered by the applets. An applet authenticates the Application Operator role by verifying possession of the Application External Authenticate (XAUT) TDES key.

5.1.2 ActivCard Applet v2 on Cyberflex Access 64k v1 Cryptographic Officers roles:

- **ActivCard Applet v2 on Cyberflex Access 64k v1 Card Security Controller (CSC) Role:** This role is responsible for managing the security configuration of the card manager and security domains. The CSC role authenticates to the cryptographic module by demonstrating to the Card Manager application that he possesses the knowledge of an OP secure channel TDES key set

stored within the Card Manager. By successfully executing the OP secure channel mutual authentication protocol, the CSC role establishes a secure channel to the Card Manager and execute services allowed to the CSC role in a secure manner.

- **ActivCard Applet v2 on Cyberflex Access 64k v1 Applet Security Controller (ASC) Role:** This role is responsible for managing the security configuration of the applets. The ASC role authenticates to the cryptographic module by demonstrating to the Applet security domain that he possesses the knowledge of an OP secure channel TDES key set stored within the security domain. The ASC role also has the privilege of resetting the PIN try counter. This is performed either by authenticating himself using the OP secure channel key set, or an Unblock PIN XAUT TDES key. Note that the protection of the reset PIN retry counter service by XAUT external authentication is optional, as the reset PIN retry counter service is always accessible with the security domain OP key set.

5.2 ActivCard Applet v2 on Cyberflex Access 64k v1 Role Authentication

The ActivCard Applet v2 on Cyberflex Access 64k v1 cryptographic module supports role authentication.

5.2.1 ActivCard Applet v2 on Cyberflex Access 64k v1 User Role Authentication

- **PIN**: this ActivCard Applet v2 on Cyberflex Access 64k v1 Card Holder role must send a Verify CHV APDU to any ActivCard applet or ACA applet to access services protected with PIN access control rules. The APDU corresponding to the applet service protected by the PIN, can access the service before the cryptographic module is removed or a reset order is sent to the cryptographic module.

- **Application External Authentication (XAUT) key**: The ActivCard Applet v2 on Cyberflex Access 64k v1 Application Operator role must prove the possession of a particular TDES key to access the PKI/GC buffer read, or update service protected with the External Authentication protocol using this particular key. An 8-byte challenge is first obtained from the applet. The application controlled by the operator encrypts the challenge with a 112-bit TDES key, and submits the resulting cryptogram to the module for verification. The APDU corresponding to the particular applet service must be sent before the cryptographic module is removed or a reset order is sent to the cryptographic module.

5.2.2 ActivCard Applet v2 on Cyberflex Access 64k v1 Cryptographic Officer Role Authentication

- **OP Secure Channel key set:** The ActivCard Applet v2 on Cyberflex Access 64k v1 Cryptographic Officer (CSC or ASC) role must prove the possession of a key set composed of 3 TDES keys. Two keys (K_{MAC}, K_{ENC}) are used to derive session keys according to Global Platform specification described in [VOPS]. The session keys ensure the confidentiality of the command payload, allow the mutual authentication of the parties and protect the APDU command integrity. A third key (K_{KEK}) is used to encrypt keys transported within the APDU command.

- **Unblock PIN External Authentication (XAUT) key**: The ActivCard Applet v2 on Cyberflex Access 64k v1 Cryptographic Officer (ASC) role must prove the possession of a particular TDES key to access the ACA Applet RESET RETRY COUNTER service protected by External Authentication with this particular key (K_{XAUT}). The host application controlled by the Cryptographic Officer role encrypts an 8-byte card challenge with K_{XAUT}, and submits a RESET RETRY COUNTER APDU that includes the resulting cryptogram for verification to the cryptographic module.

5.3 FRBB ePurse roles

The purse applet defines and recognizes four roles within the cryptographic system: Issuer, Issuer Agent, POS, Foreign POS.

5.3.1 FRBB ePurse User Roles

- **FRBB ePurse Issuer Agent**: The issuer agent has the authority to change issuer level parameters within the purse. This role is also allowed to perform debit and credit operations. This role has the privileges to be able to suppress risk management features of the purse when performing debit and credit operations.
- **FRBB ePurse POS**: The POS role is allowed to do debits and credits against the purse. All risk management features are enforced during these transactions.
- **FRBB ePurse Foreign POS**: The Foreign POS role is a special, more restrictive role that allows only debits to be performed. The debits are performed with different risk management features, which minimizes the purse issuer's risk in less controlled environments, i.e. within other issuer environments in an open system.

5.3.2 FRBB ePurse Cryptographic Officer Role

- **FRBB ePurse Issuer**: The issuer is allowed full access to the purse. This is the only role that is allowed to load keys to the purse or the purse's security domain.

5.4 Services

All purse services or APDU commands can be requested within any role. However, if the necessary role is not enabled the service will return an error.

5.4.1 Card Platform Administrative Services available to the CSC role

The following card platform services are used for the administration of the security domains, and to load applets onto the cryptographic module. This command set includes the following commands:

- **Install:** this APDU is used to instruct a security domain, or the Card Manager as to which installation/instantiation step it shall perform during an applet installation process.
- **Load:** this APDU is used to load the byte-codes of the Load File (package) defined in the previously issued INSTALL command.
- **Delete:** this APDU is used by the CSC role to delete a Load File (package) or an applet (applet instance).
- **Put Key:** using the secure channel this APDU is used to add or replace security domain key sets.
- **Set Status:** this APDU is used to modify the life cycle state of the cryptographic module or the life cycle state of an application.
- **Initialize Update:** this APDU is used to initiate an OP Secure Channel with the Card Manager or a security domain. Cryptographic module and host session data are exchanged, and the cryptographic module and host upon completion of this APDU derive session keys. However, the Secure Channel is considered open upon completion of a successful EXTERNAL AUTHENTICATE command that must immediately follow the INITIALIZE UPDATE command.
- **External Authenticate:** this APDU is used by the cryptographic module to authenticate the host, to establish the Secure Channel, and to determine the level of security required for all subsequent commands within the Secure Channel. A previous and successful execution of the INITIALIZE UPDATE command is required prior to processing this command.
- **Put Data:** this APDU is used to store or replace one tagged data object provided in the command data field.

During the secured channel opening, the command access condition is specified ('CLEAR', 'MAC', 'MAC+ENC') and an access control decision is performed on the received command.

5.4.2 Applet Administrative Services available to the ASC role

The following applet administrative services are used for configuring applet specific properties and keys.

5.4.2.1 ACA Administrative Services

The following services are provided by the ACA applets.

- **Initialize Update:** This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys.
- **External Authenticate**. This APDU corresponds to the OP secure channel specification. It is used to mutually authenticate with the Cryptographic Officer and derive the session keys for the secure channel.
- **Set Status**: This APDU is sent when the applet instance life cycle needs to be changed. The applet instance life cycle can be: SELECTABLE, BLOCKED, and PERSONALIZED.
- **Set Application UID**: This APDU is sent when the UID associated with the applet instance needs to be changed.
- **Register Applet:** This APDU registers applet instances to the ACA instance so that the access control and secure message service can be provided.
- **Register ACR:** This APDU manages the mapping between ACRID and actual APDU instruction.
- **Reset Retry Counter:** All PIN-protected services of all applet instances that are registered to the particular ACA instance are not accessible to the Card Holder when successive PIN verifications for that ID instance fail. These applets are then in a "PIN blocked" state.
    - If this APDU is protected in secure channel using Cryptographic Officer OP SC key set, it is used to set a new PIN value and recover cardholder access.
    - If this APDU is protected by AC External Authenticate protocol using the Unblock External Authentication (XAUT) key, it also can be used to set a new PIN value and recover Card Holder access.
- **Put Key:** Using the secure channel this APDU is used to enter the XAUT key used to unblock the PIN, and must be used with a secure channel. The APDU format is compliant with OP specifications.
- **Get Challenge:** This APDU is used in combination with AC external authenticate to perform an external authentication of the Application Operator in order to unblock the PIN.
- **AC External Authenticate:** This APDU is used in combination with a Get Challenge to authenticate the Application Operator using the AC external authenticate protocol.
- **Update Properties:** This APDU sets 1) a flag that indicates that the card holder must change his PIN before any PIN protected service can be accessed; 2) return either CAC v1 status word, or GSC-IS v 2.1 status word, when the Card Holder enters the wrong PIN.

5.4.2.2 PKI/GC Applet Administrative Services

The PKI/GC Applet provides RSA-based cryptographic services. Each PKI/GC applet instance can store up to eight objects, either an RSA key pair / certificate object or Tag + Length and Value buffer object.
.
The following services are provided by a PKI/GC applet instance:

- **Generate Key Pair:** This APDU is used to generate an RSA Key Pair in the cryptographic module. The Private Key is associated with a PKI Applet instance.
- **Put Key:** Using the secure channel this APDU is used to import/unwrap the private key (Chinese Remainder Theorem) components. The APDU format follows OP specification. A unique private key exists for each RSA key pair object.

- **Set Properties:** This APDU is used to set the object ID of the different PKI/GC objects in the PKI/GC applet instance. Note that the access control rule is enforced at object level rather than the instance level.
- **Read Certificate / Static Buffer:** This APDU is used to read the data from the selected buffer.
- **Update Certificate/ Static Buffer:** This APDU is used to update the data stored in the selected buffer.

5.4.3 Applet Usage Services Available to Application Operator

The following services are available to the Application Operator role:

- **Get Challenge:** This APDU is the first step of the AC External Authenticate protocol and it returns the card random challenge to the host.
- **AC External Authenticate** This APDU is the second step of the AC External Authenticate protocol and it sends the cryptogram to the card for verification of the Application Operator role on the host..
- **Read Certificate / Static Buffer:** This APDU is used to read the data from the selected buffer.
- **Update Certificate / Static Buffer:** This APDU is used to update the data stored in the selected buffer.

5.4.4 Applet Usage Services Available to Card Holder

The following services (APDUs) are common to all instances of applets:

- **Verify CHV:** This APDU checks the PIN presented by the Card Holder against the current PIN associated with the ACA applet instance.

5.4.5 Card Platform and Applet Services Available to No Role (unauthenticated)

- **Select**: this command is used for selecting an application (Card Manager, security domain or Applet). The Card Manager may be selected either for the loading of a Load File or for installing a previously loaded application (or security domain).
- **Get Data:** the GET DATA command is used to retrieve a single data object. This command is available outside of a Secure Channel (no security condition). However, if issued within a Secure Channel, it must follow the same security level as defined in EXTERNAL AUTH.
- **Get Status:** if the Card Manager is the current application, this command is used to retrieve Card Manager information according to a given search criteria.
- **Get Response:** this command is restricted to T = 0 ISO protocol for an incoming command which have data to send back. That data is received with the GET RESPONSE command sent immediately after the command it is related to.
- **PRNG Statistical Tests:** this command is used to execute the statistical tests for randomness on the on-card DRNG
- **Get Properties**: This APDU is used to obtain information about applet instance configuration.
- **Get ACR:** This APDU is used to retrieve the ACR definition for the services.
- **Get Certificate**. This APDU is used to obtain the certificate corresponding to RSA private key stored in the corresponding object.
- **Read Certificate / Static Buffer:** This APDU is used to read the data from the selected buffer.

5.4.6 FRBB ePurse Applet Administrative Services

These services are exclusively used by the Issuer role.

- **Load TLV Table:** Loads the TLV data table to the card during the priming process.
- **Put Key:** Global Platform specific command that adds keys to the cryptographic module using the secure channel.

These services are usable by either the Issuer or Issuer Agent roles.

- **Issue:** Loads cardholder specific data.
- **Prime:** Loads applet serial number and issuer specific data.
- **Put Data:** Writes data to the card.
- **Set Status:** CAC specified command that allows the status of the application to be changed.

5.4.7 FRBB ePurse Usage Services

These services are available to the Issuer, Issuer Agent or POS roles.

- **Credit:** Credits monetary value to the stored balance within the purse.
- **Initialize Credit:** Prepares the card for crediting by performing a risk assessment on the transaction.

These services are available to all authenticated purse roles.

- **Debit:** Performs the actual debiting of the balance stored within the purse.
- **External Authenticate:** Global Platform specific command that authenticates the host and determines the level of security required for all subsequent commands. Required command for establishing a secure channel.
- **Initialize Debit:** Prepares the card for debiting by performing a risk assessment on the transaction.
- **Initialize Transaction:** Allows the purse to participate in a non-financial transaction, i.e. expiry date change.
- **Invalidate Purse:** Cancels a purse and disallows it from being used for debit or credit purposes. This function zeroizes the purse transaction keys (Debit key, Credit key, Debit Signature key, Credit Signature key).
- **Sign Transaction:** Returns transaction signature and finalizes debit or credit.

5.4.8 Unauthenticated Services

Authentication is not required to access these services.

- **Get Data:** Reads data from the card.
- **Get Properties:** CAC specified command that retrieves applet instance properties.
- **Get Response:** Returns the response created by the previous command.
- **Initialize Update:** GlobalPlatform specific command that initiates the initiation of a secure channel.
- **Select:** Selects the application using its AID. P1 must be set to 0x04.
- **Verify PIN:** Sends a cardholder's PIN to the card for verification.

5.4.9 Relationship between Roles and Services: FRBB ePurse

None of the roles are configurable as to which services that they can perform.

Role / Service	Un-Authenticated	Issuer	Issuer Agent	POS	Foreign POS
Credit		✓	✓	✓	
Debit		✓	✓	✓	✓
External Authenticate		✓	✓	✓	✓
Get Data	✓[1]	✓	✓	✓	✓
Get Properties	✓	✓	✓	✓	✓
Get Response	✓	✓	✓	✓	✓
Initialize Credit		✓	✓	✓	
Initialize Debit		✓	✓	✓	✓
Initialize Transaction		✓	✓	✓	✓
Initialize Update	✓	✓	✓	✓	✓
Invalidate Purse		✓	✓	✓	✓
Issue		✓	✓		
Load TLV Table		✓			
Prime		✓	✓		
Put Data		✓	✓		
Put Key		✓			
Select	✓	✓	✓	✓	✓
Set Status		✓	✓		
Sign Transaction		✓	✓	✓	✓
Verify PIN	✓	✓	✓	✓	✓
Authentication Method	**Not Required**	**Secure Channel**	**Secure Channel**	**Secure Channel**	**Secure Channel**

[1] Not all data is available without authentication. Certain data will only be available through authenticated roles.

5.5 Service Authorization

In addition to the proper role being authenticated, certain services require additional authorization in order to perform their respective services. This authorization is achieved using a cryptogram. The cryptogram is calculated using triple DES keys and encryption. Credit and optionally debit require additional authorization.

5.6 Service Confirmation

The debit and credit services of the purse require confirmation that they actually occurred. This confirmation is achieved through the use of a cryptographic authentication code that is generated via the Sign Transaction command. Sign Transaction uses triple DES keys and encryption to generate a non-reputable signature.

6 Module Cryptographic Functions

FIPS 140-2- approved algorithms are used in the ActivCard Applet v2 on Cyberflex Access 64k v1 to provide cryptographic services. These include:

- TDES, (2 key TDES) Cert. #125
- TDES MAC Cert. #125 (vendor affirmed)
- SHA-1, Cert. #108
- RSA Sign (PKCS1 v1.5) Cert. #58
- ANSI x9.31 RNG (vendor affirmed)
- DES - ECB, CBC modes (transition phase only – valid until May 19, 2007; Cert. #179, not available for use)
- DES MAC (transition phase only – valid until May 19, 2007; Cert. #179, vendor affirmed, not available for use)

The purpose of the FRBB ePurse v2 on the Cryptographic module is to provide a FIPS approved purse that can be used within Treasury Stored Value programs. Keys are used within the mechanisms that allow role authentication and service authorization. The FRBB ePurse uses the following FIPS 140-2 approved algorithms:

- TDES, (2 key TDES)
- TDES MAC
- ANSI x9.31 RNG (vendor affirmed)

The FRBB ePurse does not rely on the DES security functions provided by the ActivCard Applet v2 on Cyberflex Access 64k v1. The module is not invalidated by the expiration of the DES transition phase.

6.1 Power-up Self Tests

The cryptographic module performs the required set of self-tests at power-up time. When the cryptographic module is inserted into a smart card reader and power is applied to the cryptographic module (contact) interface, a “reset” signal is sent from the reader to the cryptographic module. The cryptographic module then performs a series of GO/NO-GO tests before it responds (as specified by ISO/IEC 7816) with an Answer To Reset (ATR) packet of information. These tests include:

- RAM functional test & clearing at reset
- RNG functional test
- EEPROM Firmware integrity check
- Algorithm (known answer) tests for:
  - CRC16

- DES (ECB & CBC mode encrypt/decrypt, not available for use)
- TDES (ECB & CBC mode encrypt/decrypt)
- SHA-1 Hashing
- RSA PKCS1 sign and verify

If any of these tests fail, the cryptographic module responds with an ATR, and a status indication of a self-test error, and the cryptographic module goes mute. No data of any type is transmitted from the cryptographic module to the reader while the self-tests are being performed. DES is not available through the cryptographic module interface.

6.2 Conditional Self Tests

- RSA Key generation: A pair-wise consistency check is performed during key generation.
- Random Number Generator:
  - NDRNG: A 16 bit continuous test is performed during each use of the hardware non-deterministic RNG. The NDRNG is used to generate seed values to feed the DRNG.
  - DRNG: A 16 bit continuous test is performed during each use of the FIPS140-2 approved deterministic RNG.
- Software/Firmware load test:
- A TDES CBC MAC is verified each time an applet is loaded onto the cryptographic module.

7 Critical Security Parameters

7.1 ActivCard Applet v2 on Cyberflex Access 64k v1 CSPs

- **Initialization key K_{init}**: used to secure the card during its transportation from the manufacturer site to the issuance site. This is a TDES key and is replaced with the card manager OP key set as the first step of issuance.

- **Card Security Controller (CSC) OP Key Set:** This is the card manager OP secure channel key set consists of the following three keys:
  - **K_{enc}:** Triple-DES key used to derive session keys for the encrypted mode of the secure channel
  - **K_{mac}:** Triple-DES key used to derive session keys for crypto officer authentication and MAC mode of the secure channel. This key is used to authenticate the CSC role to the card
  - **K_{kek}**: Triple-DES key used to encrypt keys to be loaded onto the cryptographic module

- **Applet Security Controller (ASC) OP Key Set:** This is the security domain OP secure channel key set consists of the following three keys:
  - **K'_{enc}**: Triple-DES key used to derive session keys for the encrypted mode of the secure channel
  - **K'_{mac}**: Triple-DES key used to derive session keys for crypto officer authentication and MAC mode of the secure channel. This key is used to authenticate the ASC role to the card
  - **K'_{kek}**: Triple-DES key used to encrypt keys to be loaded onto the cryptographic module

- **Application External Authentication (XAUT) Key**: Triple-DES key that enables the authentication of Application Operators (PKI/GC read or PKI/GC Update)

- **Unblock PIN External Authentication (XAUT) key:** Triple-DES key that enables the ASC role to perform the Reset Retry Counter operation.

- **RSA private keys**: managed (generated, unwrapped) from the PKI/GC applet using the Java card cryptographic services. These keys are used to sign data.

- **Personal Identification Numbers (PIN):** PINs and PIN attributes are managed from the ACA Applet, which relies on Java Card PIN management service.

- **Authentication Method (or ACR)**: These data elements define the Authentication Method that is permanently set for the service. Several services offer a configurable Authentication Method.

7.1.1 Access to CSPs and Settings:

The following matrix identifies how different services access CSPs for each applet.

Roles and Services / Access to CSPs	Card Holder	Application Operator	Cryptographic Officer	INSTALL/INSTANTIATE (CSC)	CHANGE REFERENCE DATA	GET PROPERTIES (NO ROLE)	GET ACR (NO ROLE)	INITIALIZE UPDATE (NO ROLE)	EXTERNAL AUTHENTICATE (ASC)	VERIFY CHV (C.H)	PUT KEY (ASC)	GET CHALLENGE (NO ROLE)	AC EXTERNAL AUTHENTICATE (ASC)	SET STATUS (CSC)	UPDATE PROPERTIES (ASC)	RESET RETRY COUNTER (ASC)	REGISTER APPLET (ASC)	REGISTER ACR (ASC)
ACR																		
Install			✓	✓														
Register ACR			✓															✓
PIN																		
Reset Retry Counter			✓													✓		
Change Reference Data	✓				✓													
Verify CHV	✓									✓								
XAUT Key																		
Enter/Delete Key			✓								✓							
Verify Cryptogram		✓											✓					
OP key set																		
Enter/Delete Key			✓								✓							
Verify Cryptogram			✓						✓		✓					✓		
Decrypt APDU Payload			✓								✓					✓		
Applet Instance Status																		
Set Status			✓											✓				
Register Applet			✓														✓	
Update Property			✓												✓			

7.2 FRBB ePurse Applet CSPs

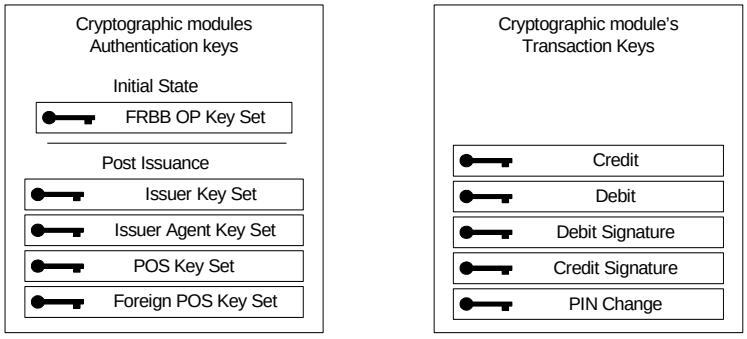

Figure 2 –FRBB ePurse v2 Security Domain, Key Distribution and Role Separation

- **Credit Key:** Triple-DES key used to calculate the credit cryptogram, which authorizes the purse to add value to the purse.

- **Debit Key:** Triple-DES key used to calculate the debit cryptogram, which authorizes the purse to reduce value.

- **Debit Signature Key:** Triple-DES key used to calculate a debit signature with a Triple-DES MAC at the completion of a transaction. The signature is used to provide proof that this card was present during the transaction.

- **Credit Signature Key:** Triple-DES key used to calculate a credit signature with a Triple-DES MAC at the completion of a transaction. The signature is used to provide proof that this card was present during the transaction.

- **Issuer Key Set:**
  - **Issuer Encryption Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Issuer MAC Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Issuer Key Encryption Key:** Triple-DES key used to provide key encryption for loading of keys into the card.

- **POS Key Set:**
  - **POS Encryption Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **POS MAC Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **POS Key Encryption Key:** Not used. Set to a randomized value.

- **Foreign POS Key Set:**
  - **Foreign POS Encryption Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Foreign POS MAC Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Foreign POS Key Encryption Key:** Not used. Set to a randomized value.

- **Issuer Agent Key Set:**
  - **Issuer Agent Encryption Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Issuer Agent MAC Key:** Triple-DES key used to form the OP Secure Channel for authentication.
  - **Issuer Agent Key Encryption Key:** Not used. Set to a randomized value.

- **FRBB OP Key Set:**
  - **FRBB OP Encryption Key:** Triple-DES Transport key used to form the initial OP Secure Channel for authentication.
  - **FRBB OP MAC Key:** Triple-DES Transport key used to form the initial OP Secure Channel for authentication.
  - **FRBB OP Key Encryption Key:** Triple-DES key used to provide key encryption for loading of the Issuer key set into the card.

- **PIN Change Key:** Not used. Set to a randomized value.

7.2.1 Access to CSPs and Settings: FRBB ePurse

A = Access: Reads value and uses it in the execution of services.
W=Write: Writes key values into memory
Z=Zeroize: Overwrites key value with randomized data.

CSP/ Keys / Roles/ Services	FRBB OP Key Set	Issuer Key Set	Issuer Agent Key Set	POS Key Set	Foreign POS Key Set	Credit Key	Credit Sign Key	Debit Key	Debit Sign Key	Pin Change Key (Not Used)
Issuer	AZ	AWZ	WZ	WZ	WZ	AWZ	AWZ	AWZ	AWZ	WZ
Issuer Agent			A			AZ	AZ	AZ	AZ	Z
POS				A		AZ	AZ	AZ	AZ	Z
Foreign POS					A	Z	Z	AZ	AZ	Z
Credit						A				
Debit								A		
External Authenticate		A	A	A	A					
Get Data										
Get Properties										
Get Response										
Initialize Credit						A				
Initialize Debit								A		
Initialize Transaction										

CSP/ Keys / Roles/ Services	FRBB OP Key Set	Issuer Key Set	Issuer Agent Key Set	POS Key Set	Foreign POS Key Set	Credit Key	Credit Sign Key	Debit Key	Debit Sign Key	Pin Change Key (Not Used)
Initialize Update		A	A	A	A					
Invalidate Purse						Z	Z	Z	Z	Z
Issue										
Load TLV Table										
Prime										
Put Data										
Put Key	Z	WZ	WZ	WZ	WZ	W	W	W	W	W
Select										
Set Status										
Sign Transaction							A		A	
Verify PIN										

8 Security Rules

8.1 Approved Mode of Operation

The cryptographic module must be operated on the following operational platform:

- FIPS 140-2 validated Axalto Cyberflex Access 64K v1:
  - OS Hardmask: n5 v1
  - OS Softmask: n4 v2

- FIPS 140-2 validated ActivCard Applet v2 (CAC framework v2.3.0C):
  - ACA applet package: v2.3.0.5
  - PKI/GC applet package: v2.3.1.2
  - ASC library package: v2.3.0.3

The operational environment must operate in the FIPS Approved mode of operation per the FIPS 140-2 validated ActivCard Applet v2 on Cyberflex Access 64K v1 module's security policy. [2] Any deviation from this operational environment invalidates the FIPS 140-2 validation of FRBB ePurse v2 cryptographic module.

[2] Reference Security Policy listed at Certificate. #418

8.2 Applet Life Cycle Security Rules

The Cryptographic module only permits loading of FIPS approved applets. Applets can only be loaded through an OP secure channel (i.e. they pass from the external application to the cryptographic module in an encrypted and MACed form).

- The Card Holder must take the necessary measures to insure that the terminal and/or Card Acceptance Device are controlled by a valid role; Card Holder, Application Operator or Cryptographic Officer / crypto-officer.
- Management of applet life cycles (load, install, delete, personalize keys) shall follow the Open Platform standard [VOP].
- Applet and key APDU command management (i.e. download, install, delete, put key) are protected by secure channel MAC (TDES-CBC). Their origin is authenticated, and their integrity verified. In particular this protects the applet byte code against tampering when downloaded at post-issuance.
- The download of validated applet packages, and the installation of applet instances, may occur either at pre-issuance, issuance or post-issuance.
- There may be as many instances of each applet as there are cryptographic module resources available.
- The issuer must take the necessary measures to insure that the terminal and/or Card Acceptance Device are controlled by a valid Crypto Officer or User role.
- Management of applet life cycles (load, install, delete, personalize keys) shall follow the Global Platform v2.0.1

8.3 Authentication and Access Control Security Rules

8.3.1 ActivCard Applet v2 on Cyberflex Access 64K v1 Authentication

- The module shall provide the following distinct operator roles: The Card Holder role, Application Operator role, Applet Security Controller role and Card Security Controller role.
- Applets shall provide role-based authentication:
    - The Card Holder is authenticated by the knowledge of a unique PIN.
    - The Crypto Officer is authenticated via OP secure channel mutual authentication protocol using the card manager/security domain key set that composed of 3 TDES double length keys. Two keys are used to authenticate and MAC the command payload. A third key is used to encrypt keys transported within the APDU command (Initialize Update & External Authenticate commands). For Crypto Officer is also authenticated via AC external authenticate protocol using the Unblock PIN XAUT TDES key.
    - The Application Operator role is authenticated via AC external authenticate protocol using the application XAUT TDES key.
- Cryptographic services are restricted to authenticated roles.
- The role authentication methods (ACRs) for each applet service are set by the Crypto Officer during applet instantiation and can only be modified by the Crypto Officer.
- When authentication of the role cannot be performed because the related key or PIN attributes are missing, the corresponding service must be disabled.
- The results of authentication must be set in transient memory and therefore cleared when the module is powered down.
- Applet instance configuration may require the combined authentication of different roles to access a particular service. For instance the Application Operator, or the Cryptographic Officer, must both authenticate to access the Update Certificate / Static Buffer service.

8.3.2 FRBB ePurse Authentication

- Authentication roles control what services can be accomplished within the purse.
- Purse operations can only be performed by authenticated devices.
- The module uses secure channel as an authentication process involving Triple-DES keys. The entity being authenticated must possess knowledge of the keys in order for the authentication process to succeed. All roles are authenticated using the secure channel.

8.3.3 Access control

- Keys must be loaded through an OP secure channel. Consequently, keys are always loaded in the encrypted form.
- The password or PIN that is used by the applet to authenticate the Card Holder must not be divulged to other parties than the Card Holder.
- The ACA applet must be configured by the cryptographic officer so that:
- After 1 <= N <= 255 consecutive unsuccessful PIN code validation attempts, the Card Holder services must be disabled. (e.g. The PIN is blocked)
    - The PIN length L verifies the following rules:
    - 6 <= L <= 255 for PIN composed with random numeric (0-9) or alpha-numeric (0-9, a - z, A – Z) characters

- The PIN that is used by the applet to authorize the Card Holder requests must not be divulged to other parties.
- The associated strength of authentication is as follows:
    - Triple-DES shared secret through Secure Channel:
        - The number of possible TDES keys (2^{112} potential key values) is greater than 1,000,000. Providing a random access rate approximately equal to one in 5.19 x 10^{33} attempts, which is less than 1 in 1,000,000.
        - The timing of the OP secure channel authentication method allows for 222 failed attempts per minute. The likelihood of a successful random attempt per minute is approximately 1 in 2.34 x 10^{31} attempts. This is less than the likelihood of one successful attempt in a 100,000, per one-minute time period.

8.4 Physical Security Rules

The physical security of the cryptographic module is designed to meet FIPS 140-2 Level 3 requirements. The cryptographic module physical boundary is comprised of an epoxy encapsulated smart card chip and micro electronic wiring, and a contact pad. The physical boundary encloses all firmware required for the performance of services offered by the module.

8.5 Key Management Security Policy

8.5.1 Cryptographic Key Generation

- Triple DES session key derivation uses FIPS 140-2 approved ANSI X9.31 DRNG for secure channel opening.
- Payment session keys use a purse maintained sequence number for establishing session keys.
- No triple DES application or role keys are generated on the card.
- The FRBB ePurse applet does not support cryptographic key generation.

8.5.2 Cryptographic Key Entry

Keys shall always be entered in encrypted format, using the Put Key command within an OP secure channel. During this process, the keys are encrypted using the necessary Key encryption key. No secret keys or private keys are output by the module.

8.5.3 Cryptographic Key Storage

The Keys are structured to contain the following parameters:

- Key ID, which is the Id of the key
- Algorithm ID, which determines which algorithm to be used
- Integrity Mechanisms.

8.5.4 Cryptographic Key Zeroization

The cryptographic module zeroizes cryptographic keys by reloading a zero-valued key set for Crypto Officer OP secure channel key set, security domain keys, Application Operator XAUT key and closing of secure channel for session keys. The cardholder PIN is zeroized by setting it to zero value. The RSA private key is zeroized by reloading a zero-valued key.

The FRBB ePurse zeroizes or destroys keys by randomizing their values using FIPS 140-2 approved ANSI X9.31 DRNG provided by the cryptographic module. The Invalidate Purse service performs this function.

9 Mitigation of Attacks

The cryptographic module has been designed to mitigate the following attacks:

- Simple Power Analysis
- Differential Power Analysis

10 Security Policy Check List Tables

10.1 Roles and Required Authentication

Role	Type of Authentication	Authentication Data
Issuer	OP Secure Channel Mutual Authentication Protocol	OP Secure Channel Triple DES Key Set
Issuer Agent	OP Secure Channel Mutual Authentication Protocol	OP Secure Channel Triple DES Key Set
POS	OP Secure Channel Mutual Authentication Protocol	OP Secure Channel Triple DES Key Set
Foreign POS	OP Secure Channel Mutual Authentication Protocol	OP Secure Channel Triple DES Key Set
Card Security Controller	OP secure channel mutual authentication protocol	OP Secure Channel Triple DES Key Set
Applet Security Controller	OP secure channel mutual authentication protocol or TDES	OP Secure Channel Triple DES Key Set or Unblock PIN XAUT TDES key
Application Operator	AC External Authenticate protocol	Application XAUT TDES key
Cardholder	Verify CHV Service	PIN

10.2 Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
TDES authentication	> 1:1,000,000
PIN	> 1:1,000,000

11 References

[JVM] Java Card ™ 2.1 Virtual Machine Specification v1.1 - June 1999, Sun Microsystems

[JCAPI] Java Card ™ 2.1 Application Programming Interface, Sun Microsystems

[JCDG] Java Card ™applet developer's guide

[JCRE] Java Card ™ 2.1 Runtime Environment (JCRE) Specification, Sun Microsystems

[VOPS] Global Platform - Open Platform Card Specification, v2.0.1' – April 2000

[VOPI] Visa Open Platform Card Implementation Specification - March 1999, Visa International

[X9.31] American Bankers Association, Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, Washington, D.C., 1998.

[FIPS140-2] National Institute of Standards and Technology, FIPS 140-2 standard.

[FIPS140-2A] National Institute of Standards and Technology, FIPS 140-2 Annex A: Approved Security Functions.

[FIPS140-2B] National Institute of Standards and Technology, FIPS 140-2 Annex B: Approved Protection Profiles,

[FIPS140-2C] National Institute of Standards and Technology, FIPS 140-2 Annex C: Approved Random Number Generators

[FIPS140-2D] National Institute of Standards and Technology, FIPS 140-2 Annex D: Approved Key Establishment Techniques

[DES] National Institute of Standards and Technology, Data Encryption Standard, Federal Information Processing Standards Publication 46-3, October 25, 1999.

[DES Modes] National Institute of Standards and Technology, DES Modes of Operation, Federal Information Processing Standards Publication 81, December 2, 1980.

[DSS] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000.